



АУДИТ РИСКОВ КИБЕРБЕЗОПАСНОСТИ

Хотите узнать источники основных угроз безопасности ваших данных?
Мы подскажем

ОСНОВНЫЕ ВЫВОДЫ:
ГРУППЫ С ГЛОБАЛЬНЫМ ДОСТУПОМ

Неограниченный глобальный доступ настроен более чем для **66,5 миллиона папок**
66 502 976 из 90 348 156

Группы с глобальным доступом
В эту категорию входят такие группы, как «Все пользователи домена» и «Авторизованные пользователи». Группы с глобальным доступом позволяют всем участникам организации получать доступ к данным на основе единых параметров управления доступом. Как правило, доступ к данным не должен предоставляться группам с глобальным доступом, таким как «Все пользователи домена» и «Авторизованные пользователи». Данные, доступные всем пользователям без исключения, более всего подвержены уязвимости, утечке, кражам или несанкционированному использованию.

Распределение глобального доступа для групп	
CFS_FS_2	11%
CFS_FS_3	7%
CFS_FS_4	20%
SP_FS_1	44%
EXCH_FS_1	18%

Конфиденциальные файлы с глобальным доступом для групп	
CFS_FS_2	2%
CFS_FS_3	1%
CFS_FS_4	2%
SP_FS_1	82%
EXCH_FS_1	13%

www.varonis.com | Образец отчета «Оценка рисков в области данных»

ОСНОВНЫЕ ВЫВОДЫ:
ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ

- 423 110 операций открытия файлов
- 182 335 операций изменения файлов
- 65 120 операций удаления файлов
- 22 965 изменений в предоставленных разрешениях

Основные категории оповещений

Вторжение	5
Превышение прав	9
Кража данных	2

Распространение конфиденциальных файлов

CFS_FS_2	13%
CFS_FS_3	12%
CFS_FS_4	8%
SP_FS_1	54%
EXCH_FS_1	13%

Более **750 000 событий** в рамках аудита
950 событий, связанных с конфиденциальными данными

Действия и поведение пользователей
Действия пользователей — это операции с данными, выполняемые пользователями внутри организации. В эту категорию входят действия с файлами и приложениями, электронной почтой и OneDrive, а также изменения параметров пользователей и роли внутри организации. Не выявлены данные о действиях, невозможном формировании шаблонов типичного поведения пользователей. Функция Мониторинг позволяет отслеживать и анализировать поведение пользователей и объектов сети и предоставляет информацию о подозрительных или необычных действиях. Эти данные используются для обнаружения отклонений от типичного поведения, а также для отправки уведомлений, выявления факторов риска, обнаружения несанкционированного использования вычислительной и сетевой ресурсов и решения других задач. Эти типы угроз являются основными источниками безопасности для большинства организаций. Возможность обнаружения, блокировки и предотвращения таких угроз — ключ к созданию надежной системы безопасности.

www.varonis.com | Образец отчета «Оценка рисков в области данных»

ОСНОВНЫЕ ВЫВОДЫ:
ОЦЕНКА ВОЗМОЖНОСТЕЙ

УРОВЕНЬ	ВОЗМОЖНОСТЬ
Полный	Оптимизация изменений в Active Directory и предоставление отчетов (численность в группе, объекты групповой политики и т. д.)
Частичный	Оптимизация изменений списка параметров управления доступом и предоставление отчетов
НП	Оптимизация использования электронной почты и предоставление отчетов (отправка, получение, «Отправить как» и т. д.)
НП	Оптимизация использования электронной почты и предоставление отчетов (отправка, получение, «Отправить как» и т. д.)
НП	Обнаружение нестандартных действий в файловой системе и электронной почте
Частичный	Анализ возможностей доступа к объектам файловых контейнеров
Частичный	Анализ возможного доступа к объектам контейнеров электронной почты
НП	Анализ возможностей доступа пользователей и групп к различным файловым контейнерам
НП	Анализ возможностей доступа пользователей и групп к различным хранилищам данных электронной почты
Частичный	Определение конфиденциального или регламентированного содержимого
Частичный	Определение устаревшего, неиспользуемого содержимого
НП	Передача утверждения запросов на доступ владельцам данных

www.varonis.com | Образец отчета «Оценка рисков в области данных»



Что включает оценка рисков кибербезопасности?

- ✓ **Определение** источников угроз, таких как избыточные права доступа, устаревшие данные и неупорядоченные разрешения, и расстановка приоритетов по уровню риска
- ✓ **Обнаружение** конфиденциальных и персональных данных с недостаточной защитой или высоким уровнем риска
- ✓ **Проверка** параметров управления доступом и процессов авторизации и поиск возможностей для оптимизации защиты
- ✓ **Анализ** прав доступа к папкам и файлам с возможностью определения зон максимального риска и снижения его уровня
- ✓ **Выявление** уязвимостей в среде ваших данных для обеспечения их безопасности

“Аудит рисков помог нам определить, какие конфиденциальные данные находятся в зоне риска и не защищены, но что более важно – сформировать пошаговый план для устранения всех уязвимостей.

Фабио Роккаталиата (Fabio Roccatagliata) | Директор по безопасности | D'Amico Societa' di Navigazione



Принцип работы

Мы находим проблемные зоны.

Беспокоитесь по поводу глобальных прав доступа? Или несанкционированного использования конфиденциальных данных? Не знаете, что делать с устаревшими данными? Мы знаем. Мы поможем вам расставить приоритеты и предложим конкретные шаги для повышения уровня безопасности данных.



Что мы анализируем?

Инженеры Varonis соберут и проанализируют метаданные вашей электронной почты, файловых систем и служб каталогов (Active Directory, LDAP, NIS), выделят соответствующие участки инфраструктуры и выполнят оценку возможностей и среды.

Для вас будет создан индивидуальный отчет об оценке системы безопасности с учетом особенностей вашего бизнеса, нормативных требований и параметров конфигурации.



Результат

Вы получите подробный отчет о состоянии данных вашей компании, содержащий анализ рисков, а также описание сильных и слабых сторон вашей системы безопасности. Кроме того, наши специалисты помогут вам решить существующие проблемы безопасности, представляющие реальную угрозу.

Отчет основан на реальных фактах и цифрах и содержит описание найденных уязвимостей, выводы и рекомендации по исправлению с указанием приоритета.



Быстро и без лишних затрат

Выделенный инженер Varonis выполнит всю необходимую работу, включая установку, настройку решения и анализ, а также подготовит рекомендации по улучшению безопасности данных.



Без ущерба для производительности

Наши действия не замедлят работу ваших сотрудников и систем. Varonis отслеживает миллионы событий в день, не влияя на производительность и бизнес-процессы.